DOI: 10.38146/BSZ.2019.1.7

BENCSIK BALÁZS

A kiberbiztonsági feladatok kezelése az európai uniós jogalkotás fényében

A XXI. században a társadalom technológiafüggősége, a digitális eszközök és technológia térnyerése olyan jelentős mértékű, hogy mára szinte behálózta az életünk mindennapi tevékenységeit, munkafolyamatait és hivatali ügyintézéseit. A kibertér térnyerésének és a digitális technológia elterjedésének köszönhetően az irodából, otthonról vagy akár útközben is elintézhetjük magán-, illetve munkahelyi feladatainkat. Ha azonban nem megfelelő körültekintéssel, nem tudatosan élünk a technológia adta vívmányokkal, számos veszélyt és fenyegetést is a fejünkre vonhatunk.

Napjainkban egyre elterjedtebbé válik a dolgok internete is (Internet of Things; IoT). Az IoT eszközök képesek kétirányú kommunikációt folytatni más eszközzel, adatokat, információkat továbbítanak nekik, a felhőalapú technológia segítségével eltárolja vagy továbbítani tudja a világ bármely részére. Az IoT technológián alapuló eszközöket okos- vagy smarteszközöknek is nevezzük. Ennek megfelelően IoT eszköz lehet a telefon, számítógép, tablet és a tévé, de ami ennél különlegesebb, hogy már olyan eszközök is felszereltek efféle technológiával, mint például az autó, a villanykörte, a hűtőszekrény vagy akár egyes orvosi eszközök.

Láthatjuk, hogy az életünk minden apró szegmensét behálózzák az okosmegoldások, az IoT technológia, ezért az adataink biztonsága érdekében nagyon fontos, hogy minden eszköz esetében törekedjünk a megfelelő és biztonságos használatra, a biztonsági beállítások körültekintő elvégzésére.

Miután pedig a kibertér az életünk minden apró területén jelen van, ugrásszerűen növekszik a sérülékenységek és támadható eszközök és rendszerek aránya. Egyre gyakoribbak az állami és a civil szektort érő kibertámadások. Világszerte évi négyszázmilliárd dollárra* becsülhető a kiberbűnözők által okozott kár a globális kibertérben.

A 2013-as Ibtv. meghatározása szerint kibertérnek nevezzük a *„globálisan összekapcsolt decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk for-*

* http://www.digitalhungary.hu/interjuk/Teged-is-megloptak/5530/

májában megjelenő társadalmi és gazdasági folyamatok együttesét". Általános jellemzője, hogy globális, folyamatosan bűvölő virtuális hálózat, decentralizáltságából fakadóan pedig egyetlen állam által sem szabályozható. Ennek következtében jelentős biztonsági kockázatokat hordoz minden egyes felhasználó számára.

Miért van szükség ilyen átfogó kiberbiztonsági programokra?

A kibertámadásoknak súlyos, a nemzetbiztonság, a gazdaság, illetve a társadalom mindennapi életét veszélyeztető következményei lehetnek. Ezt támasztja alá a Világgazdasági Fórum éves globális kockázati rangsora is, amely szerint a hagyományos veszélyek (háborús konfliktusok, terrorizmus, természeti katasztrófák stb.) mellett a kibertér fenyegetései minden évben egyre előrébb kerülnek.

A probléma olyannyira kritikus, hogy Kanada, Svédország, Norvégia, Finnország, Dánia, Hollandia, Japán, az Egyesült Arab Emírségek, Malajzia és Szingapúr is első helyen említi meg a kibertámadásokat mint amely a legnagyobb veszélyt jelenti a társadalomra és a gazdaságra.

Összetettségét jól jelzi, hogy 2015 óta a kibertámadások két legkiemelkedőbb alkategóriájának tekintjük a kiberkémkedést és az adatlopást, amelyeknek főleg a gazdasági következményei jelentősek.

Globális fenyegetések

Az Europol fenyegetésértékelése szerint megfigyelhető a kiberbűnözés és a „hagyományos" bűnözés közötti határvonal elmosódása, hiszen a bűnözők számára az internet megfelelő felület a tevékenységük kiterjesztésére, illetve további eszközöket kínál a bűncselekmények elkövetéséhez. Az internet nyújtotta anonimitás és személytelenség biztonságot ad és bátorítja a bűnözőket, illetve nagyon megnehezíti, szinte lehetetlenné teszi a nyomon követésüket és az igazságszolgáltatás elé állításukat.

A 2017. májusi zsarolóvírus-hadjárat mutatja igazán a támadás egyes ágazatokra és az országokra gyakorolt valós hatását, hiszen több mint százötven országban, több mint százkilencvenezer rendszert érintett, beleértve például a kórházak feladatait. A korábbiakban jellemző számítógépes kártevők célja

főként az adatlopás vagy a kritikus rendszerek megbénítása, valamint a zombihálózatok bővítése volt, napjainkban viszont az olyan károkozók elterjedése figyelhető meg, amelyek fájlokat tiltanak le, alkalmazásokat zárnak le, a feloldásukért pedig pénzt követelnek a felhasználótól. Az egyik ilyen kiemelkedő támadássorozat volt az elmúlt időszakban a WannaCry zsarolóvírushullám 2017 májusában, amely az elmúlt évek eddigi legnagyobb és legtöbb felhasználót és szervezetet elérő támadássorozata volt.

A vírus gyors terjedésének legfőbb oka egy a Windows minden verziójában megtalálható (az XP-től a Windows 10-ig bezárólag) sebezhetőség volt. Ez önmagában még nem lett volna elég a kártevő térnyeréséhez, ehhez jelentősen hozzájárultak a felhasználók. A Microsoft már március közepén kiadta a sérülékenység javítására szolgáló frissítést, amelynek számítógépére telepítését számos felhasználó nem engedélyezte, elhalasztotta vagy figyelmen kívül hagyta. Ennek következtében több héttel a vírus felbukkanása után még mindig jó néhány olyan Windows-alapú számítógép akadt, amelyre nem került fel a sérülékenységet kijavító és a kártevő elkerüléséhez szükséges frissítés.

A kártevő hihetetlen sebességgel söpört végig az egész világon, felmérhetetlen károkat okozva cégeknek, szervezeteknek és magánszemélyeknek.

2016 folyamán egy trójai típusú káros kód elterjedésének lehettünk tanúi, amely szintén Windows-alapú operációs rendszereket támadott. Az áldozatok bitcoinban fizetendő díj ellenében kapták meg a támadótól a kódot a saját rendszerükhöz. Hasonló támadást észleltek 2017-ben is a WannaCry-hullám után, és ez még a WannaCrynál is gyorsabban terjedt. Kéretlen leveleken keresztül jutott el az áldozatokhoz, titkosította a felhasználó merevlemezének adatait, majd a titkosított jelszót, feloldó kulcsot díj ellenében kínálta a felhasználónak. A Petya elnevezésű kártevő főként Ukrajnát támadta, onnan is indult ki a MEDoc nevű ukrán cég egyik platformjának feltörésével, a cég nevében számtalan fertőzött e-mailt küldtek, valamint a MEDoc gépéről megszerezték a felhasználóik belépési adatait. A MEDoctól így megszerzett adatokat is titkosította, és a helyreállításért, a feloldókulcsért kriptovalutát kért a támadó vírus. Aztán a szakértők gyorsan rájöttek, hogy itt már nem a pénzügyi haszonszerzés volt a cél, inkább a káoszkeltés és a gazdasági károkozás, elsősorban Ukrajnában. A Petya aktívan terjedt világszerte, így további jelentős károkat okozott még Oroszországban, Lengyelországban, Olaszországban és Németországban is.

Megfertőződött egyebek kötött a csernobili atomerőmű állapotát monitorozó rendszer, a kijevi reptér biztonsági rendszere és a kormányzati infrastruktúra is, valamint az orosz Rosznyefty egyik rendszere is. De érintett volt

az Oreót gyártó Mondelez cég, a Mars, a Nivea, valamint az OTP Bank ukrán leányvállalata is. Ekkor már egyértelmű volt, hogy ez már nem kifejezetten a Petya nevű kártevő, inkább egy pusztításra törekvő, törlő fertőzésről van szó *(wiper),* amelynek esetében nem lehet visszaállítani az adatokat, mivel a vírus „eldobja" a feloldókulcsot, az csak álca volt. Ennek a fertőzésnek a hivatalos neve PetrWrap lett.

A felhasználók és a vállalatok

Ma már mindenki tisztában van vele, hogy a kibertér lehet a modern világ új hadszíntere. Nemcsak a bűnözők, hanem egyes nagyhatalmak is egyre gyakrabban nem a hagyományos eszközökkel, hanem diszkrétebb, kibereszközökkel szereznek érvényt akaratuknak és céljaiknak, például a belső demokratikus folyamatokba történő beavatkozás útján. Egyre inkább terjednek a dezinformációs kampányok, álhírek és kritikus infrastruktúrák elleni kiberműveletek, és az eddigi gyakorlatunktól eltérő válaszreakciót igényelnek. Az új technológiák terjedése és ugrásszerű fejlődése tovább fogja gazdagítani a kibertérben rossz szándékúan, támadásra vagy befolyásolásra felhasználható eszközöket és szolgáltatásokat.

Ez is bizonyítja, hogy a digitális átalakulással és fejlődéssel egyidejűleg egyre jelentősebb és változatosabb fenyegetésekkel kell szembenézünk, ezért kiemelkedő fontosságú a megfelelő kiberbiztonsági környezet és szabályok kialakítása. Elengedhetetlen a társadalmunk és gazdaságunk számára kulcsfontosságú hálózatok és szolgáltatások vonatkozásában a megfelelő kiberbiztonsági intézkedések megvalósítása. Az e szolgáltatásokat érő támadások vagy incidensek felmérhetetlen károkat okozhatnak, valamint visszavethetik a fogyasztók új technológiák iránti bizalmát.

A veszélyeztetettséget nemcsak vállalati hálózatok és szabályok, hanem a felhasználók szintjén is szükséges kezelni, hiszen mint minden rendszerben, itt is az ember a leggyengébb láncszem. Az Eurostat 2016-os felmérése szerint az unió polgárainak a hetvenegy százaléka megosztott már online valamilyen személyes adatot. A leggyakrabban megosztott adattípusok a kapcsolattartási adatok voltak (az internethasználók hatvanegy százaléka), majd következnek a személyes adatok, például név, születési idő vagy személyi igazolvány száma (52 százalék) és fizetési adatok, például hitel-/betéti kártya vagy bankszámla száma (40 százalék).

A felmérés kimutatja továbbá, hogy az uniós állampolgárok több mint ötöde (22 százalék) szolgáltatott már ki más személyes adatokat, például fényképeket, vagy az egészségükre, a foglalkozásukra vagy a jövedelmükre vonatkozó információkat különböző online felületeken.

Az említett felmérés eredményei szerint a fiatalabb generációk könnyebben elérhetővé teszik személyes adataikat, ugyanis a 16–24 éves internethasználók több mint háromnegyede (78 százalék) osztott meg valamilyen személyes információt online, szemben a 65 és 74 év közötti felhasználók 57 százalékával.

A felhasználókon túl a vállalatoknak, szervezeteknek is modern, napjaink próbáinak megfelelő információbiztonsági technológiával és szabályrendszerrel kell bírniuk az adataik, rendszerek és dolgozóik biztonsága érdekében. Az Eurostat-felmérés az állampolgárok, azaz a felhasználók szokásain túl megvizsgálta a vállalatok digitális szokásait is. E szerint napjainkban az unióban működő összes vállalkozás (98 százalék) használ számítógépeket, és közülük csak 31 százaléknak van formálisan meghatározott informatikai biztonságpolitikája, belső szabályozása. A felméréshez Magyarországról kapott adatok szerint a kis- és közepes vállalatok mindössze kilenc százalékának volt biztonsági politikája, a nagyvállalatok esetében ez az arány ötven százalék.

Az Eurostat-felmérés eredményeiből kitűnik, hogy a biztonságos és tudatos digitális jelenlét terén még jelentős fejlődésre van szükség az állampolgárok és a vállalatok szintjén egyaránt. E cél elérésének számos módja lehet, a folyamatos oktatástól, tudatosítástól egészen a szigorú jogszabályok és ellenőrzési mechanizmusok kialakításáig.

Az unió válasza a növekvő próbatételekre

Az IKT piaca jellemzői

Jelenleg az Európai Unióban az infokommunikációs szektor alapjai döntő mértékben harmadik országokban fejlesztett és gyártott hardvereszközök, illetve szoftverek, mindez egyes területeken monopolisztikus vagy oligopolisztikus ellátási láncok kialakulásához vezetett. Ezek az infokommunikációs rendszerek ma már csak biztonságtudatos módon fejleszthetők és üzemeltethetők a kibertérben folyamatosan jelen lévő fenyegetettség miatt. A gyártói biztonságtudatosság, a számítógép-biztonsági és -incidenskezelő csoportok *(Computer Security Incident Response Team; CSIRT)* hálózata, illetve a kibervédelmi jogszabályok lehetővé teszik a kibertámadásokból adódó koc-

kázatok bizonyos mértékű kezelését. A legnagyobb probléma az, hogy a kibertérben nem érvényesül az arányosság elve: a kétszer nagyobb tűzfal nem jelent kétszer nagyobb védelmet, sőt egy apró hiba egy teljes infokommunikációs ökoszisztémát tehet ki potenciális támadásoknak a hiba javításáig, amely hónapokig is elhúzódhat.

Az infokommunikációs szektorban a termékek és szolgáltatások kiemelkedően magas innovációs tartalmának, illetve az internet globalitása miatti mobilitásnak köszönhetően kiemelkedő a gyártói koncentráció. Néhány nagyvállalat – sok esetben állami támogatás és összefonódás mellett – oligopolisztikus piacot alakított ki világszerte, ezért gyakorlatilag megkerülhetetlenné váltak az infokommunikációs rendszerek biztonságának garantálása szempontjából. E gyártók és szolgáltatók döntően nem uniós tagállamokban működnek.

Az Európai Bizottság 2017 szeptemberében átfogó, ambiciózus kiberbiztonsági csomagot bocsátott ki, amely a megnövekedett kiberfenyegetésekre, valamint az egységes digitális piac elérésének akadályaira kíván megfelelő válaszokat, mechanizmusokat és jogi garanciákat alkotni.

A kiberbiztonsági csomag magában foglalja a bizottság közleményét a felülvizsgált uniós kiberbiztonsági stratégiáról, egy jogszabályjavaslatot, az úgynevezett kiberbiztonsági jogszabályt *(Cybersecurity Act),* amely az Európai Unió Hálózat- és Információbiztonsági Ügynöksége *(European Union Agency for Network and Information Security; ENISA)* mandátumának felülvizsgálatára vonatkozik, az európai kiberbiztonsági ügynökség létrehozásával, továbbá a kiberbiztonsági tanúsítás kérdéskörével kapcsolatos rendelkezéseket. A csomag része az úgynevezett blueprintre vonatkozó bizottsági ajánlás is, amely ismerteti, hogy a kiberbiztonságot miként illesztik be a meglévő uniós szintű válságkezelési mechanizmusokba, és meghatározza a tagállamok egymás közötti, valamint a tagállamok és az illetékes uniós intézmények, szervezeti egységek, ügynökségek és testületek együttműködésének céljait és módszereit a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre reagálás terén.

Fontos kiemelni, hogy kibertérből érkező fenyegetések az egyes államok számos különböző működési területét érintik, ezért nem lehet meghatározni olyan univerzális védekezési stratégiát, amely egyaránt hatékony az infokommunikációs gyártók hibáiból eredő sérülékenységek, a bűnözői csoportok támadásai, illetve potens állami szereplők által kifejtett offenzív tevékenységek ellen. A fenyegetések potenciális hatásainak felmérése is problematikus terület, mivel nehéz rangsorolni a veszteség súlyossága szempontjából egy milli-

árdos gazdasági kémkedési ügyet, egy emberéleteket követelő ipari kiberszabotázs akciót, illetve a kibertérben a demokratikus választási rendszer befolyásolására tett kísérletet. Sajátos veszélyforrás a szuverén állam polgáraival szemben tömegesen elkövetett illegális adatgyűjtés, ami a személyes adatok megsértéséhez, sőt akár az állampolgárok döntéseinek tömeges manipulációjához, és a demokratikus értékek sérüléséhez is vezethet.

A kiberbiztonsági támadások, fenyegetések nem maradnak országhatárokon belül, ezért törekedni kell arra, hogy olyan szabályozásokat fogalmazzunk meg, amelyek nemzetközi szintűek és a világ minden részén egységesen alkalmazhatók. Ennek megfelelően a határon túli, nemzetközi együttműködés kérdéskörét is elsőrendűként kezeli a kiberbiztonsági csomag, így célkitűzésként fogalmazza meg az EU–NATO-együttműködés elmélyítését, a nemzetközi regionális és bilaterális kapcsolatokban a kiberbiztonság, válságkezelés és -megelőzés terén történő együttműködést, valamint a harmadik országokkal történő együttműködés során a kapacitásépítés támogatását és a jó tapasztalatok megosztását.

A csomag számos javaslatot fogalmaz meg a kiberbűnüldözés terén történő együttműködés, a kibertámadás elhárításának a kidolgozására, az állami és magánszektor együttműködésének elősegítésére, a kutatás-fejlesztés terén megvalósítandó együttműködésre, valamint a kiberkészségbázis létrehozására.
A továbbiakban az itt vázolt kibercsomag egyes témáit és elemeit ismertetem.

Biztonsági tanúsítási keretrendszer

Az informatika gyorsan változó iparág, egyes területein elengedhetetlenül fontos az új technológiákhoz való hozzáférés (például tudományos munkák, programozás stb.). Tagadhatatlan, hogy a kiberbiztonsági csomag egyes javaslataival az unió területén működő szervezetek némi hátrányba és időhátrányba kerülhetnek, például a tanúsítás szükségessége miatt az engedélyeztetési folyamat következtében. Mindamellett nagyon fontos a gyors változások megfelelő és állandó követése, figyelése, az azokra való felkészülés hálózatbiztonsági szempontból, hiszen az egyes biztonsági események, működésben bekövetkező sérülések, meghibásodások, továbbá a támadások jelentős hányada éppen a legújabb fejlesztések és változások miatt következik be, nem kismértékben a nem kellő védelmi felkészültség okán.

A kialakítandó tanúsítási keretrendszer célja, hogy az egységes tanúsítás bevezetésével javuljon a termékek és szolgáltatások biztonsága, tájékoztassa és meggyőzze az állampolgárokat az érintett infokommunikációs termékek

és szolgáltatások biztonsági tulajdonságairól, ezzel növelve a beléjük vetett bizalmat. Hosszú távon ez az uniós piac fellendüléséhez vezethet. A javaslat egyik ambíciója, hogy a biztonsági aspektus már a kezdeti szakaszban, a termékek és szolgáltatások tervezése és fejlesztése során is figyelembe veendő szempont legyen, így megvalósulhasson az úgynevezett „secured by design", azaz a tervezett biztonság elve.

Ezért a kiberbiztonsági csomag javaslatot fogalmaz meg a tanúsítás kérdéskörének uniós szintű szabályozására is.

Ennek megfelelően az Európai Unió egy jogszabályjavaslat keretében létrehozza az európai kiberbiztonsági tanúsítási keretrendszert az infokommunikációs termékekre és szolgáltatásokra vonatkozóan.

Az európai kiberbiztonsági tanúsítási keretrendszer általános célja annak igazolása, hogy a keretrendszer szabályainak megfelelően tanúsított infokommunikációs termékek és szolgáltatások megfelelnek a meghatározott kiberbiztonsági követelményeknek. Ebbe beletartozna például a (tárolt, továbbított vagy más módon feldolgozott) adatok védelmének képessége a véletlen vagy illetéktelen tárolással, feldolgozással, hozzáféréssel, nyilvánosságra hozatallal, megsemmisítéssel, véletlen elvesztéssel vagy módosítással szemben.

A keretrendszer létrehozása lehetővé teszi majd egyfelől, hogy az ilyen rendszerek részeként kiállított tanúsítványok minden tagállamban érvényesek legyenek, illetve minden tagállam elismerje őket, továbbá megfelelő megoldást kínálna a piac jelenlegi széttagoltságának problémáira.

Az unió kiberbiztonsági tanúsítási keretszabályozása a meglévő szabványokra hagyatkozna, azokra a technológiai követelményekre és értékelő eljárásokra, amelyeknek jelenleg minden terméknek meg kell felelnie egyes tagállamokban, és nem egy teljesen új uniós technológiai szabványt dolgoznának ki.

A jogszabály nem vezet be közvetlenül működőképes tanúsítási rendszereket, ehelyett egy úgynevezett keretrendszert alakít ki az infokommunikációs termékekre és szolgáltatásokra vonatkozó egyedi tanúsítási rendszerek (európai kiberbiztonsági tanúsítási rendszerek) létrehozásához. A bizottság felkérésére az európai kiberbiztonsági tanúsítási rendszerek kidolgozása az ENISA feladata az európai kiberbiztonsági tanúsítási csoport segítségével. Az így elkészülő tanúsítási rendszereket a bizottság fogadja el hivatalosan végrehajtási jogi aktusok által.

Az ilyen rendszereknek olyan konkrét elemet kell tartalmazniuk, mint az érintett termékek és szolgáltatások kategóriáinak azonosítása, a kiberbiztonsági követelmények részletes leírása (szabványok vagy műszaki előírások), a

konkrét értékelési kritériumok és módszerek, valamint a biztonság elérendő szintje (alapvető, jelentős vagy magas).

A javaslatban foglaltak szerint a szabályozás ellenőrzési, felügyeleti és végrehajtási feladatai a tagállamokra hárulnak. Ennek érdekében a tagállamoknak létre kell hozniuk egy nemzeti tanúsításfelügyeleti hatóságot, amelynek feladata, hogy felügyelje, a tagállam területén letelepedett megfelelőségértékelő szervezetek és az általuk kiállított tanúsítványok megfelelnek-e a rendelet előírásainak és a vonatkozó európai kiberbiztonsági tanúsítási rendszereknek. A nemzeti tanúsításfelügyeleti hatóságok illetékesek a tagállam területén letelepedett megfelelőségértékelő szervezetek által kiállított tanúsítványokkal kapcsolatos, természetes és jogi személyek által benyújtott panaszok kezelésére egyaránt.

Végül pedig a javaslat létrehozza az európai kiberbiztonsági tanúsítási csoportot, amely az egyes tagállamok nemzeti tanúsításfelügyeleti hatóságaiból áll. A csoport fő feladata, hogy tanácsot adjon a bizottságnak a kiberbiztonsági tanúsítási politikát érintő kérdésekben, és együttműködjön az ENISA-val az európai kiberbiztonsági tanúsítási rendszerek tervezetének kidolgozásában. A jogszabálytervezet szerint az ENISA feladatai közé tartozik majd, hogy ellássa az európai kiberbiztonsági tanúsítási csoport titkársági feladatait, illetve hogy a nyilvánosság számára elérhető, naprakész nyilvántartást vezessen az európai kiberbiztonsági tanúsítási keretrendszer részeként jóváhagyott rendszerekről. Az ENISA a szabványtestületekkel is kapcsolatot tartana, hogy elősegítse a jóváhagyott rendszerekben használt szabványok megfelelőségét, és hogy azonosítsa a kiberbiztonsági szabványokat igénylő területeket.

Kiberdiplomácia

A 2017 júliusában elfogadott, a rossz szándékú kibertevékenységekkel kapcsolatos közös uniós diplomáciai intézkedések uniós kerete (úgynevezett „kiberdiplomáciai eszköztár") létrehoz egy a közös kül- és biztonságpolitika keretébe tartozó intézkedésgyűjteményt, mely intézkedések az EU politikai, biztonsági és gazdasági érdekeit sértő kibertevékenységekre adott reakciók, válaszok erősítését hivatottak megvalósítani. Ez az eszköztár a bilaterális diplomáciai vagy politikai egyeztetéstől egészen a szigorú, akár gazdasági korlátozó intézkedésekig számos különböző erősségű és hatású reagálási lehetőséget fogalmaz meg. A keretrendszer fontos lépés az uniós és tagállami szintű jelző- és reagálási kapacitások fejlesztésében. Az eszköztár hosszú távon hoz-

zájárul a konfliktusok megelőzéséhez, a kiberbiztonságot fenyegető veszélyek mérsékléséhez, illetve a nemzetközi kapcsolatok stabilitásának a növekedéséhez egyaránt. Remélhetőleg az eszközök használata visszatartó erejű lesz a lehetséges agresszorok magatartására, így hosszú távon csökkenteni fogja a támadások és kiberincidenesek számát. Az eszköztár alkalmazása kapcsán kiemelendő, hogy a rossz szándékú kibertevékenységekkel szemben az „arányos reagálás" elvét szükséges betartani. A támadás állami vagy nem állami szereplőknek tulajdonítása a továbbiakban is a minden forrást igénybe vevő hírszerzésre alapított, szuverén politikai döntés marad.

Az EU–NATO-együttműködés fontossága

A kiberbiztonság kérdéskörét és a kibertérbeli stabilitás garantálását elsőrangúként kezeli az EU és a NATO egyaránt. Ennek megfelelően 2016. július 8-án sor került egy közös EU–NATO-nyilatkozat elfogadására a kiberbiztonság, a hibrid fenyegetések és védelem terén történő együttműködési célok megfogalmazására. A stratégia célja az unió és a NATO közötti együttműködés kibővítése, a párhuzamos és összehangolt EU–NATO-gyakorlatok szervezésével, illetve a kiberbiztonsági követelmények és szabványok kölcsönös átjárhatóságának megteremtésével.

A hibrid fenyegetések vonatkozásában a stratégia célja a már korábban létrejött együttműködések és közös erőfeszítések – különösen a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport és a NATO hibrid fenyegetéseket elemző csoportja közötti együttműködés – elmélyítése, élénkítése az ellenálló képesség és a kiberválságokra való reagálás erősítése érdekében.

A kiberbiztonsági vészhelyzet-elhárítási mechanizmus és a kiberbiztonsági vészhelyzet-elhárítási alap

Mivel egyes kiberbiztonsági incidensek jelentős hatással lehetnek akár a gazdaság működésére és az emberek mindennapi életére, ezért fontos megfontolni egy vészhelyzeti válságmechanizmus kidolgozását, illetve a létező biztonságpolitikai válságmechanizmusok kiberbiztonságra történő kiterjesztését.

A kibercsomag része az a tervezet is, amely vázolja a kiberbiztonsági szempontok beillesztését az integrált uniós politikai válságreagálási rendszerébe, illetve az EU általános riasztási rendszereibe.

A kiberbiztonsági aspektus válságmechanizmusokba való hatékony beillesztésén túl fontos lenne egy kiberbiztonsági vészhelyzet-elhárítási alap lét-

rehozása is, a más uniós biztonságpolitikai területeken meglévő hasonló válságmechanizmusokhoz kapcsolódó alapok példája nyomán. Az alap lehetővé tenné, hogy egy jelentősebb és átfogóbb incidens esetén vagy utána a tagállamok támogatást, segítséget kérjenek a gyors reagálás megvalósításához, vagy a vészhelyzeti válaszlépések finanszírozására.

Természetesen az alap felhasználására csak azoknak a tagállamoknak nyílna lehetőségük, amelyek az uniós előírásoknak és szabályoknak megfelelő kiberbiztonsági rendszert alakítottak ki (még az incidens bekövetkezése előtt), megfelelően végrehajtották a hálózati és információs rendszerek biztonságának az egész unióban egységesen kimagasló szintjét biztosító intézkedésekről szóló, az Európai Parlament és a tanács (EU) 2016/1148 irányelve (2016. július 6.) rendelkezéseit, illetve fejlett nemzeti kockázatkezelési és felügyeleti keretrendszerük van.

Kiberbiztonsági kompetenciahálózat
és az európai kiberbiztonsági kutatási és kompetenciaközpont

Az EU-stratégia napirendjére tűzte a kutatás- és kompetenciafejlesztés fellendítésének és uniós szinten történő koordinálásának kérdéskörét is. Alapvető cél, hogy uniós szinten fejlesszék a közösség digitális gazdasága, társadalma és demokráciája biztonsága érdekében kulcsfontosságú kritikus infrastruktúrákat és digitális szolgáltatásokat egyaránt.

Ez a kormányzati és magánszféra együttműködésével, az akadémia és a kutatás-fejlesztési területek bevonásával valósulhat meg a leghatékonyabban. A PPP-együttműködés fontosságát már a korábbi stratégiai dokumentumok is kiemelt célként fogalmazták meg. A bizottság előrejelzése szerint a köz- és magánszféra közötti kiberbiztonsági partnerség 2020-ig várhatóan 1,8 milliárd euró befektetést generál. A világ más területein ezt jelentősen meghaladja az együttműködésbe befektetett összeg. Az Egyesült Államokban például tizenkilencmilliárd dollárt szánnak a kiberkutatás-fejlesztésre a Fehér Ház által kiadott 2016. évi „kiberbiztonsági intézkedési terv" alapján.

Az Európai Unió a kiberbiztonsági képességének megerősítése céljából az uniós tagállamok kiberbiztonsági kompetenciaközpontjainak hálózatba szervezését tervezi, valamint létre szándékozik hozni a hálózat központjául szolgáló úgynevezett európai kiberbiztonsági kutatási és kompetenciaközpontot. Ez a hálózat és annak központja serkentené a kiberbiztonság területén a technológia fejlesztését és bevetését, segítené a kutatás-fejlesztési támogatások hatékony elosztását, uniós és nemzeti szinten kiegészítené a terület kapacitás-

építési erőfeszítéseit, valamint lehetőséget nyújtana nagyobb kutatás-fejlesztési projektek megvalósítására több tagállam kutatóközpontjainak közös kezdeményezéseként.

Első lépésként a bizottság a nemzeti központok hálózatba szervezését szeretné megkezdeni. A pilot projektként funkcionáló első szakaszban a Horizon2020 keretből ötvenmillió eurót fordítana a hálózat kialakítására.

A tervezet szerint a jövőben a kutatási területek a következő generációs digitális technológiák fejlesztésére is fókuszálnának, lefedve így a mesterséges intelligenciát, a kvantum-számítástechnikát, a blokkláncot és a biztonságos digitális személyazonosságot.

Kiberkészségbázis kiépítése

A 2017. évi Global Information Security Workforce tanulmány alapján előrejelzések szerint a kiberbiztonságiszakember-hiány a privát szektorban 2022-re 350 ezer fő lesz, de globális szinten elérheti akár az egymilliót is. E probléma megoldása érdekében fejleszteni kell a kiberbiztonsági oktatást. Szükség van még több kiberbiztonsági szakember képzésére, az infokommunikációs szakemberek kiegészítő kiberbiztonsági képzése, illetve új kiberbiztonsági szakképzések útján.

A szakemberek képzésén túl fontos, hogy a többi szakterület (például mérnöki tevékenység, közoktatási, menedzsment vagy jog) oktatási tervébe is be kell építeni alapvető kiberbiztonsági tananyagot, aminek célja, hogy más specifikus szakterületeken is beépüljön a jövő szakembereinek a gondolkodásába a biztonsági aspektus figyelembevételének fontossága, illetve hogy a munkájuk és mindennapi életük során tudatosan és biztonságosan mozogjanak a kibertérben.

A kiberbiztonság fontosságának megértését, tudatosítását, a kiberbűnözés veszélyeinek ismertetését, az alapvető digitális készségek és tudás elsajátítását már az általános és középiskolai tanulmányok idején meg kell kezdeni. Ez a folyamat segítheti hozzá a tanulókat ahhoz, hogy a későbbiekben tudatosan, biztonságosan és megfontoltan használhassák a digitális szolgáltatásokat és eszközöket a kibertérben.

Az Európai Unió célkitűzései között szerepel, hogy kialakít egy uniós szintű egységes portált, amelyen összegyűjti az összes tudatosításra alkalmas eszközt egy úgynevezett egyablakos rendszerben, tanácsot adva a felhasználóknak az egyes támadások, fertőzések megelőzéséhez, elkerüléséhez és észleléséhez. A portálon javaslatokat, információkat és segítséget találhatnának

a felhasználók arra vonatkozóan, hogy mi a teendő, ha valamilyen informatikai támadás áldozatául esnek, IT-biztonsági incidens elszenvedői lesznek, továbbá a portálon elérhetővé lehetne tenni az ilyen események esetében szükséges bejelentési mechanizmusok elérhetőségeit, linkjeit.

Az állampolgárok oktatása, tudatosítása, képességeinek folyamatos fejlesztése kiemelkedő fontosságú, hiszen az incidensek 95 százalékát valamilyen szándékos vagy nem szándékos emberi tévesztés, hiba vagy figyelmetlenség idézi elő. Ezért fontos felismernünk és minden szervezetben és természetes személyben tudatosítanunk, hogy a kiberbiztonság mindannyiunk felelőssége. Ennek megfelelően a személyes, vállalati és közigazgatási szinten egyaránt egy olyan figyelmes és tudatos magatartásnak (kiberhigiénés szokásrendszernek) kell kialakulnia, amikor is minden résztvevő megérti az aktuális fenyegetéseket, és megfelelő eszközei és képességei vannak a támadások felismerésére és a hatékony védekezésre.

Az uniónak és a tagállamoknak kiemelt fontosságúként kell kezelniük a kiberbiztonsági tudatosítást, a tudatosság fejlesztését. Ezt javasolt megvalósítani kifejezetten az iskolák, az egyetemek, az üzleti közösség és a kutatási szervek számára kidolgozott célzott tudatosító kampányok idején. Az kibercsomag célja az ENISA által 2012 óta minden év októberében tartott kiberbiztonsági hónap kampány (ECSM) folyamatos bővítése és frissítése annak érdekében, hogy a kampány mindig az aktuális trendekre és fenyegetésekre hívhassa fel az állampolgárok figyelmét, illetve hogy minél szélesebb közönséget tudjon hatékonyan megszólítani. A tudatosítás témakör esetében fontos felhívni a figyelmet az online félretájékoztató kampányok és a közösségi médiában megjelenő álhírek káros hatásaira. A tagállamoknak közösen, a meglévő tapasztalataikat egymással megosztva kell szembenézniük ezekkel a nehézségekkel, egyebek között a 2019-es európai parlamenti választásra való felkészülés kapcsán.

Összegzés

A digitális technológia megállíthatatlan fejlődése és a kibertér életünk minden területére történő kiterjedése megállíthatatlan folyamat. Ez a fejlődés számos lehetőséget és egyben veszélyt is hordoz magában.

A fejlődést nem lelassítani vagy megállítani kell, hanem meg kell próbálni ahhoz alkalmazkodni, kihasználni a benne rejlő lehetőségeket és előnyö-

ket. Nagyon fontos, hogy ebben az új, fejlett digitális technológiával teli világban megtanuljunk biztonságosan és magabiztosan mozogni.

Ennek megvalósítása érdekében az államoknak, vállalatoknak, fejlesztőknek, gyártóknak, szolgáltatóknak, állampolgároknak/felhasználóknak, sőt még a nemzetközi szervezeteknek, közösségeknek is fel kell ismerniük a szerepüket és felelősségüket.

Az Európai Bizottság által megfogalmazott kibercsomag-koncepció számos kulcsfontosságú, egymásra épülő és egymást kiegészítő intézkedést azonosított.

Sajnos nem elég a szigorú jogszabályok megalkotása, ellenőrzése és szankcionálása ezen a területen, hiszen a kiberbiztonság megteremtése és fenntartása az információbiztonságban érintett valamennyi szereplő közös felelőssége, és ennek megvalósítása elképzelhetetlen a felek együttműködése nélkül.

IRODALOM

https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

http://www.digitalhungary.hu/interjuk/Teged-is-megloptak/5530/

https://www.enisa.europa.eu/publications/european-cyber-security-month-2017

http://ec.europa.eu/eurostat/cache/infographs/ict/

https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

https://mno.hu/belfold/vilaghodito-utjara-indult-petya-a-zsarolovirus-2405259

https://kiberhonap.hu/

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

https://pcworld.hu/pcwlite/ujabb-durva-zsarolovirus-pusztit-europaban-es-amerikaban-230639.html

http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#hide/fn-1

JOGSZABÁLYOK

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”) szóló rendelettervezet

Ellenálló képesség, elrettentés, védelem: az unió erőteljes kiberbiztonságának kiépítése vonatkozásában. Az Európai Parlament és a tanács közös közleménye.
http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

Az Európai Parlament és a tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről.
http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU

A tanács következtetései a kiberdiplomáciáról, 2015.
http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf

A tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről, 2017.
http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf